One Identity Safeguard

特権アクセスを安全に保存、管理、記録、分析する

はじめに

ハッカーはシステムやデータへのアクセスを得るために、絶えずその手法を進化させています。彼らの最終目的は、特権アカウントにたどり着くことです。最近目立っている侵害のほぼすべてが、特権アカウントへの不正アクセスによって重要なシステムとデータへのアクセスを得たというものです。適切なソリューションを導入すると、安全かつ効率的に、準拠した方法で特権アカウントにアクセスすることが可能になり、侵害による損害を制限できます。

ITマネージャにとって、こうしたすべてにアクセスできるアカウントの管理は課題です。これには、膨大な数の特権アカウント、およびこれらのアカウントへのアクセスを必要とする多数のユーザなど、数多くの理由があります。その上、従来の特権アクセス管理（PAM）ソリューションには、複雑なアーキテクチャ、時間を要する導入時間、労力のかかる管理要件が伴います。

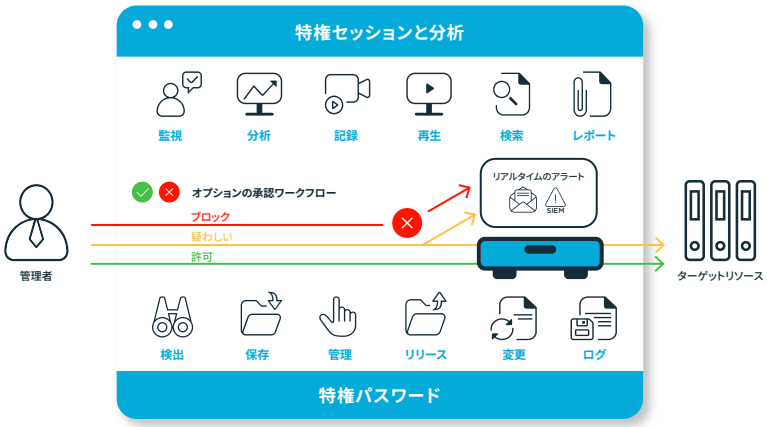
PAMは大きな課題になり得えますが、必ずしもそうである必要はありません。One Identity Safeguardは、セキュアで堅牢なパスワード保存機能と、脅威検出/分析機能を備えたセッション管理/モニタリングソリューションを組み合わせた統合ソリューションです。特権アクセスの安全な保存、管理、記録、および分析を行います。

メリット

- **セキュリティ侵害**による損害の可能性を軽減
- **コンプライアンス要件への対応**
- **シンプルな導入と管理**で迅速なROIを実現
- **効率的な監査レポート作成**
- **リスクのある行動**および通常でないイベントを識別して阻止
- **特権アカウント管理を簡素化**

妥協することなく特権アクセスを安全に保護

One Identity Safeguardを使用して、管理者と監査担当者が満足できるような特権アクセスの安全な保存、管理、記録、分析を行い、特権アカウント保護についてのストレスをなくしましょう。



Safeguard for Privileged Passwords

One Identity Safeguard for Privileged Passwordsでは、ロールベースのアクセス管理と自動化ワークフローによって、特権資格情報を付与するプロセスが自動化、制御、保護されます。

ユーザを重視して設計されているため、短期間で習得できます。さらにこのソリューションでは、どこからでもほぼすべてのデバイスからパスワードを管理できます。その結果、企業が安全に保護され、特権アクセスを持つユーザに新しいレベルの自由と機能がもたらされます。

Safeguard for Privileged Sessions

One Identity Safeguard for Privileged Sessionsでは、管理者、リモートベンダー、およびその他のハイリスクユーザの特権セッションを、コントロール、監視、記録することができます。セッション中のユーザのアクションは記録され、インデックス付けされるため、セッションイベントを簡単に見つけることができます。また、レポート作成の簡素化と自動化に役立つため、監査およびコンプライアンス要件への対応が容易になります。さらに、Safeguard for Privileged Sessionsは、プロキシとして機能してアプリケーションレベルでプロトコルトラフィックを検査し、プロトコル違反のトラフィックをリジェクトすることが可能です。そのため攻撃に対する効果的な保護となります。

Safeguard for Privileged Analytics

One Identity Safeguard for Privileged Analyticsではユーザ行動分析を利用できます。これにより、未知の内外脅威を検出し、疑わしいアクティビティを発見して阻止することができます。

脅威の潜在的なリスクレベルを評価して優先順位を付けることで、最も急を要する脅威への迅速な対応が可能になり、データ漏洩を防ぐことにつながります。

特長

ポリシーベースのリリース管理

モバイルデバイスに対応するセキュアなWebブラウザを使用し、特権パスワードとセッションへのアクセスを要求して承認を行うことができます。これらの要求は、組織のポリシーに基づいて自動的に承認したり承認の多重化を義務付けたりすることが可能です。要求者のIDとアクセスレベル、要求の送信日時、要求対象のリソース（特定のリソースだけか全部か）など、ポリシーで検討すべき独自のニーズに合わせてOne Identity Safeguardを設定できます。さらに、理由コードの入力やチケット発行システムとの統合も可能です。

全セッションを監査、記録、再生

全セッションのアクティビティ（キーストローク、マウスの動き、表示ウィンドウなども含む）がキャプチャ、インデックス付けされ、改ざん防止の監査証跡に保存されます。ここでは動画再生やデータベースのような検索が可能です。セキュリティチームは、全セッションから特定のイベントを検索し、検索条件に一致したポイントから記録を再生することができます。監査証跡は、フォレンジックとコンプライアンス目的で暗号化されてタイムスタンプが押され、暗号署名が行われます。

ONE IDENTITY by Quest

インスタントに起動

Safeguard for Privileged Sessionsは、ユーザワークフローへの変更を必要としない、トランスパレントモードでの導入が可能です。プロキシゲートウェイとして機能するSafeguardは、ネットワーク内のルーターのように、ユーザおよびサーバから見えない状態で作動することができます。管理者は、使い慣れたクライアントアプリケーションの使用を続けられ、日々の作業を中断することなくターゲットのサーバおよびシステムにアクセスできます。

ユーザ行動のバイオメトリック

各ユーザは特有の行動パターンを持っています。これは、キーボード入力やマウスの動きなどの一見どの人も同じように思えるアクションについても同様です。Safeguard for Privileged Analyticsに組み込まれたアルゴリズムでは、これらの（Safeguard for Privileged Sessionsによってキャプチャされた）行動特性を検査します。キーストロークダイナミクスとマウス動作の分析は、侵害の識別に役立ち、途切れることのないバイオメトリック認証の機能も果たします。

多要素認証のサポート

パスワードへのアクセスを他のパスワードで保護するだけでは不十分です。Safeguardに二要素認証を要求することでセキュリティを強化します。Safeguardは、RADIUSベースのあらゆる2FAソリューションをサポートします。

Safeguard for Privileged PasswordsはSAML 2.0 Web ブラウザSSOプロファイルをサポートしているため、さまざまなIDプロバイダのSTSサーバおよびサービスとのフェデレーション認証を設定し、そのMFAを使用することができます。

特権アカウントには、認証要素としてTOTP認証機能により生成されたコードが必要です。 Safeguard Privileged Passwordsは認証機能として働き、資格情報/セッションのチェックアウトと共に関連するコードを提供することができます。

パーソナル・パスワード・ボールト

無料のパーソナル・パスワード・ボールトを使えば、全従業員が、フェデレーションされていないビジネスアカウントに対するランダムなパスワードを生成して保存することができます。組織は、パスワードをセキュアに共有してリカバリできる、認可済みのツールを使用できるようになります。これにより、ビジネスアカウントに必要不可欠なセキュリティと可視性がもたらされます。

お気に入り

頻繁に使用するパスワードにログイン画面から素早くアクセスできます。複数のパスワード要求を1つのお気に入りにグループ化すれば、1回のクリックで必要なアカウントすべてにアクセス可能になります。

検出

ネットワーク上の特権アカウントまたはシステムを、ホスト/ディレクトリ/ネットワーク検出オプションを使用して迅速に検出します。

リアルタイムのアラート機能とブロック機能

Safeguard for Privileged Sessionsによってトラフィックがリアルタイムで監視され、特定のパターンがコマンドラインまたは画面上に表示されると、さまざまなアクションが実行されます。事前定義のパターンには、テキスト志向のプロトコル内でリスクを伴うコマンドまたはテキスト、あるいはグラフィカル接続での疑わしいウィンドウタイトルなどがあります。ユーザによる疑わしいアクションが検知されると、Safeguardによってイベントの記録とアラートの送信が行われ、直ちにそのセッションは終了されます。

コマンドとアプリケーションコントロール

Safeguard for Privileged Sessionsは、コマンドとウィンドウタイトルのブラックリストとホワイトリストの両方に対応しています。

広範なプロトコルサポート

Safeguard for Privileged SessionsはSSH、Telnet、RDP、HTTP、ICA、VNCの各プロトコルに完全対応しています。さらに、セキュリティチームは、管理者用に有効/無効にしたいプロトコル内のネットワークサービス（例: ファイル転送、シェルアクセスなど）を決定することができます。

フルテキスト検索

光学式文字認識（OCR）エンジンでは、セッションコンテンツでユーザが閲覧したコマンドおよびテキストの両方について、監査担当者によるフルテキスト検索が可能です。

また、ファイル操作をリストし、レビュー用に転送ファイルを抽出することもできます。セッションコンテンツとメタデータを検索できる機能によって、フォレンジックとITトラブルシューティングが迅速化され簡素化されます。

簡単な導入

迅速なアプライアンスベースの導入およびシンプルなトラフィック再ルーティングを利用するため、One Identity Safeguardでは、ユーザが作業を中断することなく、数日でセッションを記録できるようになります。

RESTful API

Safeguardは、他のアプリケーションおよびシステムとの接続にREST準拠の刷新されたAPIを使用します。各機能はAPIを介してアクセス可能となり、目的やアプリケーションの使用言語を問わず、迅速かつ簡単な統合が可能です。

変更管理

時間に基づく変更、前回の使用に基づく変更、手作業による変更、強制的な変更など、設定できる細かい共有資格情報の変更管理をサポートします。

One Identity製品による特権アクセス管理

One Identityのポートフォリオには、業界で最も包括的な一連の特権アクセス管理ソリューションが含まれます。また、オープンソースのsudoをエンタープライズ対応にするアドオン、UNIXのルートアクティビティ用のキーストロークロギングなど、UNIXのルートアカウントとActive Directoryの管理者アカウントの権限をきめ細かく委任できるOne Identity Safeguardのソリューションを活用できます。これらはいずれも、業界をリードするActive Directory連携ソリューションと緊密に統合されています。

One Identityについて

One Identityは、お客様がサイバーセキュリティ全体の体制を強化し、ビジネスに欠かせない人員、アプリケーション、およびデータを保護することを支援する、統一IDセキュリティソリューションを提供します。当社の統一IDセキュリティプラットフォームは、クラス最高のIDガバナンスと管理（IGA）、アクセス管理（AM）、特権アクセス管理（PAM）、およびActive Directoryの管理（ADMgmt）の機能を統合し、組織がIDセキュリティに対して、断片的なアプローチから包括的なアプローチに移行できるようにします。One Identityは世界中の11,000超の組織で5億を超えるIDを管理し、全世界の実績と信頼を得ています。詳細については、www.oneidentity.comをご覧ください。

ONE IDENTITY by Quest